

Fast-track Study

Trusted Services and PKI

Survey Questionnaire

August 15, 1999

Section 1

General Information

Please Note:

Completed questionnaires should be returned by Friday 27th August 1999 to:

Ray Kavanagh

Ray_Kavanagh@cmod.finance.irlgov.ie

Postal address: Centre for Management & Organisation Development
Department of Finance
Lansdowne House
Lansdowne Road
Dublin 4
Ireland

Telephone: +353 1 6045060

Fax number: +353 1 6682182

Respondent Details

Name: Richard A. Guida

Organisation: Chair, Federal PKI Steering Committee
(<http://gits-sec.treas.gov>)
Member, Government Information Technology
Services Board (<http://gits.gov>)

Address: [Room C105, 1425 New York Avenue NW](#)
[Washington, D.C. 20405](#)

Country: USA

Telephone: 202-622-1552

Fax: 202-622-9147

E-mail: richard.guida@cio.treas.gov

Section 1 (contd)**General Information**

Section 2

Strategic plans for Trusted services and PKI

- i. **To what extent does government consider a PKI necessary to deliver government services?**

- **Present**

Purpose	Essential	Highly desirable	Desirable	No requirement
Authentication		XXX		
Confidentiality		XXX		

- **Future**

Purpose	Essential	Highly desirable	Desirable	No requirement
Authentication	XXX			
Confidentiality	XXX			

Further Comments:

Level of “desirability” depends upon service(s) being supplied; for some, PKI is considered essential, for others, desirable to highly desirable, and for some, unnecessary (e.g., downloading blank forms for people to use in making applications or filing taxes)

- ii. **What policies/strategies are in place that address your government's own use of PKI?** (List and provide copies or URLs)

Details:

Basically, Federal agencies are employing public key technology in growing numbers for their own specific applications without central direction, owing to their general autonomy. The Federal PKI Steering Committee (which I chair) endeavors to help agencies learn from the experiences of others, and employ products and practices which will ultimately lead to interagency interoperability, and interoperability between the Federal government and its trading partners (e.g., state and local governments, and companies). The Steering Committee comprises over 50 members from over 24 agencies; participation is voluntary. One can describe the overall strategy as building a PKI from the bottom up – which can result in rapid growth but significant challenges later with respect to interoperability. We are working to ameliorate the latter as the former occurs.

Useful URLs are: <http://gits.gov>, and <http://gits-sec.treas.gov>. At the latter URL you can download a copy of Access with Trust, a report prepared last year on this matter but now a bit out of date. At <http://gits.gov>, you can get a copy of Access America, Vice President Gore's report on efforts to deliver electronic services to members of the public, with security and authentication being important elements. Additionally, at <http://gsa.gov>, you can get information on the General Services Administration Access Certificates for Electronic

Services (ACES) effort aimed at deploying free certificates to members of the public to facilitate electronic transactions with Federal agencies.

Section 2 (contd)

Strategic plans for Trusted services and PKI

- iii. **Has a taskforce(s)/group(s) been established to resolve issues and implement plans?**

Yes/no ...Yes.....

Please provide details for each taskforce/group and indicate the level of participation in the table provided.

a. Title: Federal PKI Steering Committee

- Participation**

All levels of government	Central government only	Government in partnership with private sector	*Other
			XXX

- Details:**

The Steering Committee comprises only Federal employees. It has three working groups (Legal and Policy, Business, and Technical), with the last (Technical) allowing participation by private industry. Participation in the other groups is limited to Federal employees under the Federal Advisory Committee Act. There is also a fourth group, the Canada/US PKI Liaison Group which focuses (as the name implies) on cooperative efforts between the Canadian Government and the U.S. Government. There is no formal group established for PKI coordination with State and local governments; that is usually done by individual agencies on an application by application basis. However, on occasion, the Steering Committee will work with State organizations (e.g., the National Association of State Information Resource Executives) directly.

b. Title:

- Participation**

All levels of government	Central government only	Government in partnership with private sector	*Other

- Details:**

.....
.....
.....

c. **Title:**

- **Participation**

All levels of government	Central government only	Government in partnership with private sector	*Other

- **Details:**
.....
.....
.....

Section 3

Key drivers for the introduction of PKI in Government

- i. **What are considered to be the key policy and business drivers behind establishing a PKI for government?**

Please illustrate 5 drivers in order of importance:

- (a) (most important) the need for strong authentication over open networks, to reduce the potential for unauthorized access (“hacking”) by remote malicious parties
- (b) Interoperability between agencies and with trading partners (other mechanisms, like PINs/passwords, interoperate poorly)
- (c) Scalability which results in cost savings in the long term
- (d) Extensibility (a PKI, once established, can be used for multiple applications, again resulting in cost savings in the long term)
- (e) Providing a single infrastructure to support both authentication and privacy/confidentiality needs

Section 4

The legal basis for the use of electronic signatures and electronic documents

- **Stage of development**

- i. **Using the following table, please indicate the stage of development of the legal basis for acceptance of electronic signatures?**

	Yes/no	Target Dates
Study of Legal Position		
• Planned		
• In progress		
• Complete	XXX	
Legislation		
• Planned		
• Proposed		
• In place/enacted	XXX	

Comments/details:

These answers require substantial elaboration.

First, for transactions between citizens or companies and the Federal government, Congress enacted legislation called the Government Paperwork Elimination Act in October 1998, which: (a) required (in most cases) agencies to receive forms in electronic form with electronic signatures (which may include digital signatures, PINs, passwords, biometrics, or digitized signatures) by October 2003; and (b) asserted that electronic signatures shall not be denied legal effect simply because they are in electronic form. The Act required the promulgation of guidance by the Office of Management and Budget on electronic signatures; draft guidance was promulgated for public comment in March 1999 (see <http://gits-sec.treas.gov>), and final guidance will be issued by April 2000. While this legislation has compelled agencies to move forward with electronic forms/signatures, there remains substantial concern within the Justice Department over the enforceability of electronic signatures in criminal cases owing to the lack of case law and the perceived complexities of explaining public key technology to a judge or jury in a persuasive fashion. On the other hand, for applications which are unlikely to involve potential criminal prosecution but instead may implicate civil litigation, there is general support for digital signature use.

Second, for transactions between private parties (e.g., contracts), over 30 States have enacted their own statutes covering digital or electronic signatures, and those statutes are in many respects very different and often inconsistent. Pending before Congress in the current session is legislation which would seek to redress that situation by establishing a Federal standard that would apply to digital signatures for such transactions, and allow States to

enact their own legislation as long as it was consistent with that standard, but there is considerable debate over whether such a provision unduly infringes on the rights of States to control commerce within their borders. Prospects for this legislation being enacted are unclear.

Finally, the question of legal acceptability of digital signatures depends a great deal, of course, on whether the matter at hand is of a civil or criminal nature. In a civil setting in the U.S. system of jurisprudence, a preponderance of the evidence is enough to prevail in a contract dispute or tort claim, for example. In a criminal case, the prosecutor must prove beyond a reasonable doubt that the indicted individual is guilty – a much tougher standard which, as indicated above, gives the Justice Department some pause.

- **Coverage and legislative approaches**

- ii. **Please indicate the overall approach to the scope and coverage of legislation in the following table and describe details of each aspect under the headings that follow:**

	`Blanket coverage` (e.g. Electronic Commerce Bill)	Incremental changes to the law	Legal precedent	Other*
Electronic signatures				Xxx
Electronic certificates				Xxx
E-contracts				Xxx
E-mail / E-documents				Xxx
*Other				

*If other please specify:

See below; impossible to categorize because of divergent approaches depending upon civil/criminal case dichotomy, and variations among State law.

Section 4 (contd)

The legal basis for the use of electronic signatures and electronic documents

- **Electronic signatures**

Comment on the legal admissibility of digital signatures and give dates of existing and planned.

General opinion is that electronic signatures in Federal cases will be legally admissible; there appears to be no bar to their admission in the Federal Rules of Civil or Criminal Procedure. Cases brought under State law, however, will vary depending upon State statutes, almost all of which vary.

- **Electronic certificates**

Comment on aspects of the use of electronic certificates and the liability of service providers

Certification Authorities (CAs) providing certificates to the general public over the internet set forth their terms and conditions which, when a subscriber purchases his or her certificate, limit liability as described. Certificates issued by companies for specific customer groups (e.g., banks) likewise have described limits of liability, but in those cases, Federal regulations may limit subscriber liability depending upon the nature of transaction. For example, if a transaction involves a credit card, the holder is limited to \$50 liability (subject to some limitations such as timely notification of theft or loss of the card) regardless of what other liability provisions may exist pertaining to a digital certificate.

- **E-Contracts**

Comment on the evidential value of electronic signatures and burden of proof in court

As set forth above, preponderance of the evidence is required to prevail in a civil case (e.g., contracts), so the evidentiary value of electronic signatures will hinge upon the standard elements of: (a) intent of the signing parties; (b) other forensic evidence; and (c) specific provisions of the contract (e.g., did it specifically allow for or require acceptance of electronic signatures, and if so, were they done in the prescribed form)?

- **Email / E-documents**

Comment on the requirements as to form (i.e. requirements for documents to be in paper form)

Because of the Government Paperwork Elimination Act (see above), electronic signatures for transactions with the Federal government are supposed to have full legal effect. However, there is no case law as yet, and concerns remain (as set forth above) about how judges and juries will react to this new technology. It is the opinion of many, however, that explaining this technology to a judge or jury is no more difficult than explaining other technical matters in cases involving environmental issues, medical evidence, or the like, where expert witness are routinely called upon to support one position or another.

- **Other**

.....
.....
.....
.....
.....

Section 4 (contd)

The legal basis for the use of electronic signatures and electronic documents

III. Does legislation specify technical solutions or approaches?

Yes/no No – GPEA focuses on “technology neutrality” among different electronic signature alternatives, instead instructing agencies to employ the technology appropriate for each application. Thus, the application, and the risks inherent in that transaction, dictate which technology is to be used – digital signatures, PINs, etc. This means agencies have considerable discretion.

If yes, please provide details of specified technical solutions:

Details:

.....

.....

.....

.....

Section 5

Government's requirement for secure services

- **Present**

- i. **Does government already utilise a standards-based interoperable system of PKI?**

Yes/No: No.

- ii. **On what technologies and standards is the PKI based ?**

See answers above; agencies select PKI products based on their specific needs and requirements, and the Steering Committee works to help ensure those selections will ultimately result in an interoperable Federal-wide PKI. Our approach to that is to design and build a Federal Bridge Certification Authority (FBCA) which will operate as a non-hierarchical hub to which agency CAs can connect (cross-certify) allowing interoperability among all agency CAs that are so connected. The Bridge is being designed now with initial operation planned for early 2000. It is intended to support interoperability among all CA products and services; there is no plan or intention to encourage or require agencies to use a single product or service.

Generic service areas

iii. What types of generic services does government already offer which use electronic certificates / signatures?

(Tick all that apply, give relevant URLs for published documents)

Generic Service	Yes / No	Relevant URL
E-commerce (purchase of government goods & services by citizens and business)	No – employ instead credit cards for purchases over SSL connections	
E-payment (tax payments, payment of government grants)	No – but plan is to use digital signatures in future	
E-filing of private information <ul style="list-style-type: none"> by citizens by businesses/enterprises 		
	No – but possibly in future for some applications (e.g., loans)	
	No – but possibly in future for some applications (e.g., loans)	
E-lookup of private information <ul style="list-style-type: none"> by citizens by businesses/enterprises 		
	No – but likely in future to check retirement and other info	
	No – but likely in future to check on information re: applications previously made	
E-notification / E-certification (notification of expiry of licences, permits, etc./ electronic delivery of licences, permits)	No – but possibly in future	
Collaborative working across government Intranets (secure E-mail and/or authenticated access to shared repositories)	Limited but growing	
Others		

Section 5 (contd)

Government's requirement for secure services

Generic service areas (contd)

If others, please specify

.....
.....
.....

Specific service applications

iv. For what specific applications does government already provide electronic services which use electronic certificates/signatures?

(Tick all that apply)

Services	Yes / No	Relevant URL
Passport applications	No	
Driving Licence applications	N/A (no Federal drivers licenses; states do this)	
Tax services	No but plan is to do in future	
Social Security services	No but plan is to do in future	
Business/enterprise registration	No but plan is to do in future	
Electronic tendering/procurement	Already done in limited areas, and growing	
Changing personal details	Already done in some agencies, and growing	
Other services		

In each case above, please provide details of:

- a) The name of the project/service;
- b) how electronic signatures are used;
- c) the infrastructure used (i.e. Internet, Intranet, other networks etc);
- d) the take-up of the service.

Details:

See <http://gits-sec.treas.gov> which will in the near future have a page describing the efforts of each Federal agency on these topics.

Section 5 (contd)

Government's requirement for secure services

- **Future**

Generic Services

- i. For what types of generic services (and timescales) is government likely to require electronic certificates / signatures in the future?

Generic Service	Estimated Implementation		
	1 year	3 years	5 years
E-commerce (purchase of government goods & services by citizens and business)			N/A – credit cards expected to continue to be used
E-payment (tax payments, payment of government grants)			Possibly within this time frame
E-filing of private information <ul style="list-style-type: none"> • by citizens • by businesses/enterprises 			
		Possibly	
		Possibly	
E-lookup of private information <ul style="list-style-type: none"> • by citizens • by businesses/enterprises 			
		Likely	
		Likely	
E-notification / E-certification (notification of expiry of licences, permits, etc./ electronic delivery of licences, permits)		Possibly (e.g., environmental permits)	
Collaborative working across government Intranets (secure E-mail and/or authenticated access to shared repositories)	Already done in limited areas; growing		
Others			

Details:

Important qualification is that question states “when is gov’t going to REQUIRE (emphasis added) e-sigs etc.” Answer is to that question is “not in the foreseeable future.” Rather, my answers are premised on the question “when will gov’t ACCEPT e-sigs etc.” GPEA is a good example – it requires the Federal government to accept electronic forms/signatures but does NOT require members of the public or companies to do so – they can still use paper forms/written signatures if they wish. Additionally, note that the question presumes “e-commerce” equates to purchasing action rather than procurement actions more generally; we will likely continue to use credit cards for purchases but for procurement actions involving contract placement, digital signatures are already being used in a limited fashion and that use is expected to grow.

Section 5 (contd)

Government's requirement for secure services

Specific service applications

- ii. For what types of specific services (and timescales) is government likely to require electronic certificates / signatures?

(Tick all that apply)

Services	Estimated Implementation			
	1 year	3 years	5 years	Not known
Passport applications				xxx
Driving Licence applications				N/A
Tax services			xxx	
Social Security Services		xxx		
Business/enterprise registration		xxx		
Changing personal details		xxx		
Electronic tendering/procurement	xxx			
Other services				

Please provide details (with information source URLs) of planned projects as indicated above:

Details:

Same proviso as above re: "required" vs. "accepted"

- iii. Have any decisions been made on standards and technologies?

Details:

Three guiding principles: (a) use of open versus proprietary standards; (b) use of the proper technology best suited to the specific application (i.e., private keys in hardware tokens are needed for some applications, but not all; in other cases, private keys on hard disks suffice); and (c) conformance (by Federal agencies) to Federal Information Processing Standards (FIPS) promulgated by the National Institute of Standards and Technology for cryptographic modules, digital signature algorithms, and the like, and to requirements set forth by NIST regarding how products are certified or shown to be in conformance with those standards. In some cases, individual agencies (e.g., the Department of Defense) impose additional requirements – such as compliance with the Common Criteria – on products they purchase.

Section 6

The provision of trust services

Certificates

- **Present**

- i. **Which organisations currently issue electronic certificates (utilising a standards-based interoperable system of PKI) potentially suitable for use in government applications?**

Organisation	Tick all that apply	Remarks
Government	Limited but growing (see GSA ACES effort cited above)	
Banks	Limited	
Post offices	Limited (electronic postage)	
Telecoms operators	No	
Internet Service Providers (ISPs)	No	
Others		

If others, please specify:

Presume this question is focused on certificates for the general public. For certificates issued to Federal agency employees, that is done either by the agency itself running its own PKI, or securing certificates under contract from a service provider or contractor.

- ii. **What identity checks are undertaken by these organisations before certificates are issued?**

Very application dependent. For members of the public, see ACES. For agency employees, depends upon application and agency (e.g., is the certificate to be used for accessing the individual's payroll account, or for signing contracts worth millions of dollars?).

- iii. **What types of media are used to store certificates / private keys?**

Smart cards	Floppy diskettes	PCMCIA cards	Removable hard disks	Others
xxx	xxx	xxx	xxx	Xxx (fixed hard disks)

If others, please specify:

Section 6 (contd)

The provision of trust services

- iv. Does government accept electronic certificates issued by multiple providers on a national basis?

Yes/No: No – but see GSA ACES effort described previously.

Details:.....
.....
.....
.....

- v. Does government accept electronic certificates issued by providers from other countries?

Yes/no No.

Details:..
.....
.....
.....
.....
.....

• Future

- vi. Who will issue electronic certificates utilising a standards-based interoperable system of PKI for use in government applications?

(Tick all that apply)

Government	Yes
Banks	Possibly
Post offices	Possibly (for postage)
Telecoms operators	No
Internet Service Providers (ISPs)	No
Others	

If others, please list:

Section 6 (contd)

The provision of trust services

- vii. **Will government accept electronic certificates issued by multiple providers?**

Yes/No/Not yet decided: Possibly for some applications

Certification

- viii. **How does an organisation establish itself as a Certification Authority(CA)/Trusted Third Party (TTP)?**

There are no specific requirements at the Federal level. In some States (e.g., Utah and Washington), licensing by the State Government is required or encouraged pursuant to State law.

- ix. **What obligations are placed on CAs/TTPs by government?**

Again, none at the Federal level (other than by contract when an agency secures such services); at the State level, it varies from State to State.

- x. **Who is, or will be, responsible for licensing Certification Authorities?**

Government (statutory regulation)	Private sector (industry self regulation)	Both	No licensing envisaged
Federal – No; State - varies	Yes in many states		

Please describe the approach that is / will be taken in the accreditation and licensing of CAs:

At the Federal level, this will be done on an agency by agency basis initially, with the expectation that guidance will be prepared to help agencies do this appropriately for the services/products they employ. In the private sector, this depends upon State by State statutes and regulations which vary.

Section 7

Barriers to the introduction of a PKI in government.

Please note that the information provided here will be used for statistical purposes only and will not be attributable to individual countries

- i. Please rank the following issues to reflect the extent to which they represent a barrier to implementing a standards-based interoperable PKI.

(Note: 1 = largest barrier)

	Rating	Remarks
Funding	1	While long term cost savings are likely, up front costs can be considerable and can deter investment
Legislation	6	At Federal level, not a significant problem owing to GPEA
Policy	2	The need to develop and implement policy often is critically underrated; there is little guidance (at present) on how to do this
Regulation	5	
Privacy/Security	7	
Standards	3	Lack of interoperability in present products is problematic
Technical Issues	4	Lack of full conformance to standards in many products is problematic (e.g., revocation status checking is rare)
Other	2	Tied with policy is ability to make PKI work with legacy data bases and directories; need strong directory support in particular (to discover certificates), but that is often lacking for reasons unrelated to PKI. Also, as separate "other," the need to train users, administrators, and staff on the use of their certificates/private keys is significant challenge; would rate that as tied with "standards" in significance hierarchy.

If other, please provide details:

Again this rating depends upon which PKI we are talking about. The rating I have given is premised upon PKI usage for intra-agency, interagency, and agency to trading partner

transactions. For transactions with the general public, then the privacy element becomes more pronounced.

Authentication

The process of reliably determining the identity of a communicating party.

Certification Authority (CA)

A Certification Authority vouches for public keys and the details of who owns them. A Certification Authority electronically signs (certifies) these details with their own private key and the resulting product is called an electronic or digital certificate.

Confidentiality

Confidentiality ensures that data is not revealed or disclosed to unauthorised persons. It is achieved through the use of encryption techniques.

Electronic certificate

An electronic certificate, or digital certificate, binds an entity's (citizen, business) public key and one or more attributes relating to its identity. The certificate provides assurance that the public key belongs to the identified entity and that the entity possesses the corresponding private key.

Electronic signature

An electronic signature, or digital signature, is an electronic analogue of a written signature in that can be used to assure a user that a document was, in fact, signed by the person who claims to have signed it (i.e. authentication). However, unlike its written equivalent, it can also prove that the content of an electronic document has not been altered (i.e. it provides assurance of integrity).

Electronic documents

The electronic equivalent of documents held in paper form.

Electronic contracts

The electronic equivalent of a contract in paper form.

E-certification

Electronic issue of licences and permits to citizens and businesses.

E-commerce

Selling of products by government agencies over the Internet e.g.

- government publications (books, maps);
- non-personal services;
- public information e.g. national statistics, Land Registry searches.

Here the authentication of clients is not a requirement i.e. they do not need electronic certificates to conduct business in this context.

E-filing

Electronic filing of personal/private information by citizens and businesses.

E-lookup

A facility for citizens and businesses to electronically examine/lookup private information held on them by government agencies.

E-payment

The receiving and/or making of payments by government agencies, citizens and businesses, for example:

- the payment of grants and benefits electronically by government agencies and their reception by citizens and businesses;
- the payment of taxes and fees electronically by citizens and businesses and their reception by government agencies.

E-notification

Electronic notification to citizens and businesses of government information, rules, procedures and also reminders concerning the expiry of licences and permits.

E-procurement/tendering

Conduct of the procurement process by electronic means:

- electronic dissemination of tender documents;
- reception of proposals in electronic form;
- seeking and receiving clarification by electronic means;
- electronic notification of outcome of procurement process to tenderers.

PKI

A PKI, or Public Key Infrastructure, is required for the widespread adoption of public key technology. A PKI consists of the following elements:

- electronic certificate holders who own public/private key pairs;
- trusted bodies called Registration Authorities who vouch for the identity of the certificate holders;
- Certification Authorities (CAs) who issue electronic certificates and provide information on the status of certificates through the maintenance of certificate revocation lists (CRLs);
- Trust relationships between CAs who recognise (cross-certify) each others certificates as a basis for extending trust.

Trusted Third Party (TTP)

(see Certification Authority)